Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (currently amended) A method for verifying a check, comprising:

scanning, at a point-of-sale location, the check to obtain data from MICR line of the check, the data including a one-way hash value;

obtaining, at the point-of-sale location, customer-specific information that is not included on the check;

providing, from the point-of-sale location to a check verifier, the scanned data and the customer-specific information;

receiving, by the check verifier, a [[the]] key from a source other than the point-of-sale location;

computing, by the check verifier, a one-way hash value based on a specific hash algorithm, the data from the MICR line, the customer-specific information, and the key; and

determining, by the check verifier, if the computed one-way hash value is the same as the one-way hash value obtained from the MICR line of the check.

2. (currently amended) The method according to claim 1, wherein the one-way hash value of the check is included in [[an]] an n-digit field at one end of the MICR line.

3. (currently amended) A check verification system, comprising:

a check printer adapted to print checks based on information provided thereto, the information including a MICR line that includes an ABA number of a bank and a customer account number,

wherein the check printer is further adapted to print the information on the MICR line based on information provided from a bank, the information including an

n-digit personal code that is not printed on the check and a [[an 1 bit]] key that is not printed on the check, and

wherein a p-bit hash value is provided on the MICR line based on the information provided from the bank.

4. (original) The check verification system according to claim 3, wherein the MICR line further includes a value corresponding to a check number.

5. (currently amended) The check verification system according to claim 3, further comprising:

a check verifier adapted to verify checks based on the information on the MICR line provided to the check verifier by an entity desiring authentication of a check presented for payment, along with the [[I-bit]] key provided to the check verifier,

wherein the check verifier is further adapted to computer a hash value for the check based on the information on the MICR line, along with information not on the MICR line that is separately provided to the check verifier by the bank.

6. (currently amended) A computer program product comprising a computer useable medium having computer program logic recorded thereon enabling a processor to create a self authenticating check, by a method comprising:

creating a payor field on a face of the check;

creating a payee field on the face of the check;

creating a check amount field on the face of the check; and

creating a MICR line on the face of the check, said MICR line including:

an n-digit ABA number;

an m-digit customer account number;

a p-digit check number; and

an r-digit one-way hash value, and

wherein the r-digit one-way hash value is computed by the computer executing a one-way hash algorithm that uses the ABA number, the customer account

number, the check number, a c-digit personal identification code that is not included on the MICR line, and a [[q-bit]] key that is not included on the MICR line.

7. (previously presented) The computer program product according to claim 6, wherein the method further comprises printing the r-digit one-way hash value at one end of the MICR line on the face of the check.

8. (previously presented) The computer program product according to claim 6,

wherein said MICR line further includes a t-digit product code value that provides information regarding an account from which the check is to be drawn against, and

wherein the r-digit one-way hash value is computed by the computer based in part on the t-digit product code.

9. (currently amended) The check verification system according to claim 3, further comprising:

a check verifier adapted to verify checks based on the information on the MICR line provided to the check verifier by an entity desiring authentication of a check presented for payment, along with the [[l-bit]] key provided to the check verifier,

wherein the check verifier is further adapted to compute a hash value for the check based on the information on the MICR line, along with information not on the MICR line that is separately provided to the check verifier by the entity desiring authentication of the check presented for payment.

10. (currently amended) A check verification system, comprising:

an apparatus adapted to selectively provide information usable by a check printer to print a p-bit hash value on a MICR line of a check, wherein the information includes:

an ABA number of a bank,

a customer account number,

an n-digit personal code that is not printed on the check, and

a [[an 1-bit]] key that is not printed on the check.

11. (previously presented) The check verification system according to claim 10, wherein the MICR line further includes a value corresponding to a check number.

12. (currently amended) The check verification system according to claim 10, further comprising:

a check verifier adapted to verify the check based on the information on the MICR line provided to the check verifier by an entity desiring authentication of the check when presented for payment, along with the [[1-bit]] key provided to the check verifier,

wherein the check verifier is further adapted to compute a hash value for the check based on the information on the MICR line, along with information not on the MICR line that is separately provided to the check verifier by a bank.

13. (currently amended) The check verification system according to claim 10, further comprising:

a check verifier adapted to verify the check based on the information on the MICR line provided to the check verifier by an entity desiring authentication of the check when presented for payment, along with the [[1-bit]] key provided to the check verifier,

wherein the check verifier is further adapted to compute a hash value for the check based on the information on the MICR line, along with information not on the MICR line that is separately provided to the check verifier by the entity desiring authentication of the check presented for payment.

14. (previously presented) The check verification system according to claim 10, wherein the system is to be operated by a bank.

15. (new) An apparatus, comprising:

a monetary instrument having a surface; and

a magnetic ink character recognition (MICR) line applied to the surface of the monetary instrument, said MICR line comprising:

an ABA number,

a customer account number, and

a one-way hash value, wherein said one-way hash value is output from a one-way hashing process using input including the ABA number, the customer account number, a personal identification code which is not included on the MICR line, and a key which is not included on the MICR line.

16. (new) The apparatus of claim 15, wherein the key is a 128-bit key.

17. (new) The apparatus of claim 15, wherein the monetary instrument is a personal check, a business check, a traveler's check, a money order, or a cashier's check.

18. (new) The apparatus of claim 15, wherein the MICR line further comprises an auxiliary onus field.

19. (new) The apparatus of claim 15, wherein the MICR line further comprises a check number and the one-way hashing process further uses, as input, the check number.

20. (new) The apparatus of claim 19, wherein the MICR line further comprises a product code number.

21. (new) The apparatus of claim 20, wherein the product code number indicates that the monetary instrument is authorized to a maximum dollar value.

22. (new) The apparatus of claim 20, wherein the product code number indicates NSF (not sufficient funds) protection.

23. (new) The apparatus of claim 19, wherein the one-way hashing process outputs a significantly different one-way hash value in response to minor changes in its inputs.

24. (new) The apparatus of claim 19, wherein the one-way hashing process uses a Cryptographic Hash Algorithm (CHA).

25. (new) The apparatus of claim 19, wherein the one-way hash value is a 6-digit number.

26. (new) The apparatus of claim 19, wherein the one-way hash value is located in a field at one end of the MICR line.

27. (new) A method comprising:

generating a one-way hash value using a one-way hashing process based on a key, a personal identification code, an ABA number, and a customer account number; and

printing a magnetic ink character recognition (MICR) line on a monetary instrument, wherein the MICR line comprises the ABA number, the customer account number and the one-way hash value.

28. (new) The method of claim 27, wherein the key is a 128-bit key.

29. (new) The method of claim 27, wherein the generating of the one-way hash value is further based on a check number, and the MICR line further comprises a check number.

30. (new) The method of claim 29, wherein the one-way hashing process uses a Cryptographic Hash Algorithm (CHA).

31. (new) The method of claim 29, wherein the one-way hashing process outputs a significantly different one-way hash value in response to minor changes in its inputs.

32. (new) The method of claim 29, wherein the generating of the one-way hash value is further based on a product code number.

33. (new) The method of claim 29, wherein the one-way hash value is a 6-digit number.

34. (new) The method of claim 29, further comprising, before using the key, decrypting an encrypted version of the key to generate the key.

35. (new) The method of claim 34, wherein the decrypting uses a 3DES algorithm.

36. (new) A method, comprising:

generating a one-way hash value using a one-way hashing process based on a key, a personal identification code, an ABA number, and a customer account number associated with a monetary instrument; and

comparing a printed one-way hash value and the one-way hash value to determine an authenticity of the monetary instrument.

37. (new) The method of claim 36, wherein the key is a 128-bit key.

38. (new) The method of claim 36, wherein the generating of the one-way hash value is further based on a check number associated with the monetary instrument.

39. (new) The method of claim 38, wherein the one-way hashing process uses a Cryptographic Hash Algorithm (CHA).

40. (new) The method of claim 38, wherein the one-way hashing process outputs a significantly different one-way hash value in response to minor changes in its inputs.

41. (new) The method of claim 38, wherein the generating of the one-way hash value is further based on a product code number associated with the monetary instrument.

42. (new) The method of claim 38, wherein the one-way hash value is a 6-digit number.

43. (new) The method of claim 38, further comprising, before using the key, decrypting an encrypted version of the key to generate the key.

44. (new) The method of claim 43, wherein the decrypting uses a 3DES algorithm.

45. (new) The method of claim 38, further comprising an issuing a status message based on an output of the comparing.

46. (new) A computer-readable medium containing instructions for controlling at least one processor by a method comprising:

generating a one-way hash value using a one-way hashing process based on a key, a personal identification code, an ABA number, and a customer account number; and

printing a magnetic ink character recognition (MICR) line on a monetary instrument, wherein the MICR line comprises the ABA number, the customer account number and the one-way hash value.

47. (new) A computer-readable medium containing instructions for controlling at least one processor by a method comprising:

generating a one-way hash value using a one-way hashing process based on a key, a personal identification code, an ABA number, and a customer account number associated with a monetary instrument; and

comparing a printed one-way hash value and the one-way hash value to determine an authenticity of the monetary instrument.